Authentification of the Origin and Content of Paperless Transactions and Questions of Liability in Continental Law part 1

Thunis, Xavier; Amory, Bernard

Published in:
International Computer Law Adviser

Publication date:
1988

Document Version
Publisher's PDF, also known as Version of record

FRANCE/BELGIUM

Authentication of the Origin and Content of Paperless Transactions and Questions of Liability in Continental Law: Part 1

BY BERNARD AMORY & XAVIER THUNIS

Introduction

After an agreement is realized between the parties to a contract, disputes may arise. For example, a party to the agreement, or even a third party, may contest the existence of the agreement itself. Since the essence of the agreement is contested, the party relying on the agreement must prove that it was actually concluded and is legally enforceable. The dispute may also relate to the identity of the parties to the agreement, if one of the parties denies having entered into the agreement in question. Less radically, some provisions of an agreement may be questioned. In such a case the problem is to define its content and meaning.

Two main questions arise: *who* has agreed? and *what* have they agreed to? The latter question not only relates to the problem of interpretation of agreed-upon provisions, but also to the scope of the contract itself. These two issues (the origin and the content of agreements) are not new. Indeed, in 1804 the authors of the Civil Code had already answered them by asserting the superiority of written evidence in respect of legal acts and that a signature permits, in principle, the signatory to be deemed the author of the legal act.

Technical progress in the audiovisual techniques of telecommunications and computer science will probably not eliminate paper entirely, but their influence is and inevitably will be more important to the legal community, which must reexamine the relevance of its present categories and perhaps create new ones. For example, the combination of computers and telecommunications (known as "telematics") allows the processing and transmission of data over long distances. Legal and scientific data bases are available to a user located thousands of miles away. The S.W.I.F.T. network,[1] electronic funds transfers, and more generally all "telematic contracts," are examples of applications of the above-mentioned techniques.

A lawyer is more interested in the intangible aspect of such transactions than in their variety. This intangibility has two aspects. First, the object of the transmission, *i.e.*, the information, is always intangible (while the means of transmission may have a tangible character, *e.g.*, the transmission of information on paper). Second, the transmission itself can now be performed without *any* long-term fixation and without incorporation of the information on paper or any other tangible medium.

These two extremes of intangibility are not new. However, because telematics both increases considerably the speed of data transmission and the possibilities of concluding contracts at long distance without any durable or tangible medium, existing problems of evidence are multiplied. Applying the old laws of evidence to new techniques raises a number of problems. The first part of this article will examine these problems of evidence and possible solutions to them, with particular attention to the authentication of acts that lack a written signature.[2]

In the second part of this article, we will examine questions of liability in paperless transactions[3] and, more particularly, in financial transactions. We will see that because of the large number of parties involved in a typical telematics transaction, the identification of the cause of damages is often difficult. The technical complexity of such a transaction suggests that we should deal with liability questions in terms of risk instead of fault.

Finally, the fact that liability and evidence questions are dealt with in the same article is not coincidental. The determination of the burden of proof and admissibility of evidence influences the rights of the parties. One should also note that the concept of "continental law" is used restrictively, since the legal analysis in this article is done principally from the standpoint of French and Belgian private law.

Authentication of computer-aided commercial transactions

The operations[4] of an enterprise can be categorized into one of two groups:[5]

- *inter-enterprise operations,* such as contracts, orders, confirmations of orders, payment instructions, etc. (hereafter referred to as "commercial transactions"), and
- *intra-enterprise operations* memorialized in documents such as inventory records and those prepared to comply with the

requirements of accounting, tax, or customs regulations.

Only the first group of operations will be dealt with in this article.

Paper documents have long been used, and are still often used, to record both inter-enterprise and intra-enterprise operations. Their advantages are well known: they can be transmitted easily, they can be stored for a relatively long period of time, they cannot easily be forged, and if attempted, alterations can be detected. Due to these qualities, paper documents are used to store data, and thereby perform an *information* function. If they comply with certain requirements, they can also serve as proof of the data they contain (*probative* function).

Furthermore, some paper documents incorporate the rights attached thereto, so that they represent these rights. These documents then have a *symbolic* function as well.[6] Bills of lading, bills of exchange, and documentary credits are examples of documents having a symbolic function.

Authentication belongs to the probative function. It has two complementary purposes—first, to identify the author of the document; and second, to indicate his willingness to appropriate the contents of the message or document.[7] As stated by the United Nations Commission for International Trade Law (UNCITRAL), "in the event of a dispute, authentication is in this respect a probative element."[8] Authentication, therefore, can be used to provide evidence of a commercial transaction, *i.e.*, to demonstrate, both to the parties to the agreement and to third parties, that a transaction has been concluded between the parties, and the content of that transaction.

Since handwriting skills are no longer limited to the élite, authentication is traditionally performed through a handwritten signature, sometimes combined with the intervention of a notary or other public officer.[9] However, as UNCITRAL has stressed, the requirements of modern business have caused many legal systems to authorize a signature appended with a stamp, symbol, facsimile, perforations, or other mechanical or electrical device.[9bis] For example, French Law nº 66-380 of June 16, 1986, relating to the use of certain automatic procedures to append signatures on commercial documents and cheques has partially confirmed the legality of the practice of signing certain commercial documents with a stamped signature or facsimile.[10]

In Belgian law, some legal provisions authorise by way of exception the use of a stamped signature (*e.g.*, for the signature on shares and bonds of the directors of a company or for the signature on notes by the National Bank). There are also certain practices which dispense with handwritten signatures altogether. One of these is insurance contracts signed by the insurer through a stamped or printed signature. These practices seem to be *contra legem*.[11]

Finally, in international law, certain treaties contain provisions which permit the use of electronic devices as signatures as long as they are not incompatible with the domestic law of the country involved.[12]

Those devices which have been permitted, in certain cases, to replace the handwritten signature are inapplicable to telematics transactions, *i.e.*, those which occur through the combined use of computers and telecommunications, because they require the physical presence of their owner and cannot be appended at long distances. Telematics creates the need for new authentication techniques adapted to its own characteristics.[13]

Section I.B below contains a non-exhaustive list of these devices and a brief description of each. Section I.C examines the legal requirements under Belgian and French law for authentication and business practices in this respect. Prior to this, Section I.A describes an international electronic fund transfer transaction, and highlights the points at which authentication is required. We stress the implications of intangibility on authentication, which is inherent in the processing and transmission through automated means, and also examine their impact on the value of proof ("the faith" pursuant to the Civil Code) one can give to intangible commercial transactions with regard to both their origin and their content. We do not, however, examine the implications of intangibility on the symbolic and purely informative functions discussed above.

A. Authentication in an international electronic funds transfer

The banking community was one of the first sectors to be computerized. Thanks to the ability to connect parties through telecommunications lines, the computers of the bank and of its customers can make a payment to another business entity without the use of any traditional written documents. Electronic funds transfers[14] provide excellent examples of authentication. The chart at the end of this article describes an international electronic funds transfer and highlights the various points of authentication.

In this transaction, a company located in Brussels (company A, transferor) makes a payment to its supplier in Paris (company C, transferee). The transaction is performed without any traditional paper documentation. The transferor and the transferee are respectively linked to their banks through an electronic system of cash management. Such a system enables company A to transmit a payment instruction to its bank A through their computers without the use of paper, since they are linked together through telecommunications lines.

Company C, which enjoys the same kind of equipment, will be able to look at its account at a distance through its computer terminal linked by telecommunications lines to the computer of its bank B, and therefore can verify if the amount paid by company A has been transferred into its account.

Since the intermediary banks are members of the international interbank network S.W.I.F.T. (Society for Worldwide Interbank Financial Telecommunications), the carriage of the message (the payment instruction) will be handled by this network and will be performed in compliance with the standards and procedures (notably in respect of authentication) of this network. Since banks A and B have a direct relationship, the settlement of the transaction will be performed between themselves with a debit of bank A's account with bank B.

If the beneficiary (company C) has an account at bank B, the latter will be able to settle the transaction in crediting company B's account. If the beneficiary does not have an account at bank B but has one at another bank which has an account relationship with bank B, the transaction will be settled between these two banks through their own means of communications.

However, in this example, if the beneficiary of the payment is domiciled at bank C with which bank A has no direct account relationship, the settlement of the transaction will be performed through a network and a clearing house of which both banks B and C are members.

In this example, since banks B and C are located in France, there will be transfers on the accounts they must have at the Banque de France. This operation can be initiated and performed in a completely intangible fashion through S.A.G.I.-T.T.A.I.R.E. (Système Automatique de Gestion Intégrée par Télétransmission de Transactions avec Imputation de Règlements Etrangers) and C.C.M.B. (Centre de Commutation de Messages Bancaires).[15] Bank B, which has received via S.W.I.F.T. the instruction to pay the beneficiary domiciled at bank C, will transmit by teletransmission to the Banque de France the instruction to debit its account and to credit bank C's account at this institution. Then, Banque de France will notify bank C of this credit. Bank C will credit the account of the beneficiary who will be able to learn of this immediately through long distance access to its accounts.[16]

In the rather complex transaction described above, there appear four points of *authentication:*

1. Company A, transferor, should authenticate itself vis-à-vis its bank A pursuant to the procedure agreed upon between themselves, so that bank A is confident that it is authorized to debit company A's account;

2. To transmit the message to bank B via the S.W.I.F.T. network, bank A should authenticate itself pursuant to the procedures of this system, *i.e.,* vis-à-vis the S.W.I.F.T. regional processor and vis-à-vis the addressee, bank B;

3. To transmit the message to bank C and to perform the settlement of the transaction via the SAGITTAIRE-CCMB system, bank B should authenticate itself vis-à-vis the Banque de France pursuant to the procedures provided for in this system;

4. Finally, to have access to his account at bank C, company C, beneficiary of the payment, should authenticate itself vis-à-vis bank C pursuant to the procedures agreed upon between themselves.

B. Modern techniques of authentication

There are three main categories of techniques of authentication: (i) password (or passnumber), also known as "secret code," which is often combined with a magnetic card, (ii) cryptography, and (iii) recognition of physical characteristics.[17]

Generally speaking, authentication means in most cases verification.[18] A machine compares the information it receives with a reference, and under certain rules it decides if the difference between them is small enough to deem that the person in question is actually the one he/she claims to be.

A verification procedure is also applied in the traditional form of authentication. Indeed, a handwritten signature is subject either to a comparison by the addressee with a specimen for reference (*e.g.,* verification of the signature of the drawer by the employee of the bank when a bearer check is presented for payment), or when the parties are engaged in a regular business relationship between them, a comparison by one party with the image it has more or less consciously built up of the signature of the other party. Verification can also be performed under a procedure specifically set out in the juridical code.

Compared to visual verification of a handwritten signature, modern techniques of authentication have the advantage of automatic and systematic verification for each transaction. However, most of the modern techniques of authentication are not infallible. Since their function is to verify the extent of a possible difference between the obtained information and a reference, and not the equality between these factors, there is always a risk of error. Each technique, therefore, should define its "threshold of acceptation," taking into account that the lower this threshold is set, the greater the risk that an authentic document will be refused by the machine (the rate of true refusal is high). On the other hand, the higher this threshold, the greater is the risk that fraudulent documents will be accepted (the rate of untrue acceptance is high).[19]

Practice has shown that the various techniques of authentication described above are at least as reliable as the handwritten signature.

Secret code

One of the most widespread techniques of authentication is authentication through a secret code.[20] The secret code is composed of a combination of figures (and/or letters) which, in principle, is unique and which is known only to its owner (that is why it is also called a "Personal Identification Number", or "P.I.N."). The secret code is often combined with the use of a magnetic card or memory card. This combination allows verification of the validity of the code without the latter remaining with a machine controlled by a third party.[21]

The secret code is largely used for authentication in electronic funds transfers, systems for the general public (transactions at automatic teller machines and point of sale terminals) and for access to databases. It is also used in electronic cash management systems for companies, at least for purely informative services (such as accessing account status). Operations involving the transfer of funds are subject to more sophisticated forms of authentication.

However, secret codes provide a high level of security. For example, in a system allowing only three unsuccessful attempts to get through and with a secret code of four figures, a fraudulent person has only a 0.03% chance to discover the secret code.[22] This technique has several drawbacks:

- a high level of risk of loss
- the owner forgetting the code, and
- successful access to the system by any fraudulent person who discovers the code.

Cryptography

Cryptography is a technique by which text is encoded with confidential keys and complex mathematical processes (algorithms) to make it incomprehensible to any person who gains access to it without the means of decoding it, *i.e.*, to put it in a readable format through a symmetrical operation.[23]

As recalled by D. Syx,[24] one generally distinguishes between two categories of cryptographic techniques: symmetrical systems and non-symmetrical systems.

In symmetrical systems, the sender and the receiver of the message use the same key to code and decode the message. These systems do not allow the performance of the various functions of authentication since each party has the same key.

On the other hand, cryptographic systems which are non-symmetrical (also known as "public key systems") are able to perform all these functions. They are based on a double key: a public key and a corresponding secret key, which allow a double operation of cryption-decryption. In order to send a message, the sender first codes it with the public key of the addressee, which he can find in a specialized directory. Then, he recodes the message with his own secret key. The addressee decodes the message first with his secret key and secondly with the public key of the sender.

Electronic cash management systems for enterprises have recourse to non-symmetrical cryptography, at least for transactions requiring a high level of security (such as payment instructions).[25] The S.W.I.F.T. network provides confidentiality through a system of symmetrical encryption and authentication through a "log-in" procedure. Pursuant to this procedure, members of S.W.I.F.T. have a "log-in table" (which is itself confidential and composed of two complementary parts transmitted by separate mail and regularly replaced). To authenticate itself, the bank issues a log-in message to the regional processor. If the secret numbers contained in the message get through the S.W.I.F.T. control procedures, a log-in acknowledgment together with another secret number is addressed by S.W.I.F.T. to its member. The latter then checks the validity of this number in view of its log-in table.

In addition to its authentication vis-à-vis the S.W.I.F.T. network, the bank which sends the message must also authenticate itself vis-à-vis the addressee bank. This authentication ensures that the received message has not undergone any accidental or fraudulent alteration and that it originates from its true sender. The calculation of the authenticator by the addressee bank and the control thereof by the addressee bank are performed by a combination of a fixed authentication number and the total number of characters contained in the message.[26]

Although they provide a high level of security, public key cryptographic systems have important drawbacks: they are expensive to install and the authentication procedure is relatively slow.

Physical characteristics

There are numerous techniques to recognize physical characteristics at a distance, but most of them are still in an experimental stage. There are, for example, the recognition of iris, sweat, walk, pace, morphology, blood, hair, etc. Apart from the technical difficulties, which must still be solved before these techniques become workable, from a legal standpoint, these techniques are unable to perform both functions of authentication (*i.e.*, identification and indication of willingness of appropriation). They only allow recognition, which is identification.

To perform the second function, they should be combined with a deliberate act by the identified person, whereby he indicates his willingness to appropriate the message (*e.g.*, in the case of recognition through the iris, the obligation to put his eyes at a predetermined place). A technique which is already workable and which fulfills both functions is dynamic recognition of the signature, *i.e.*, "the authentication of a person through the movement of his pen when he signs."[27] This

system is based on the computer's using different criteria (speed, pressure, acceleration, etc.) to compare a signature of reference kept in its memory and the signature appended by the person who seeks to authenticate himself. Although these systems are highly reliable, they are not yet extensively used.

Compared with other modern techniques of authentication, those based on the recognition of physical characteristics have a considerable advantage. They permit the identification of a determined natural person who carries out the operation, rather than only the person who has access to the network.

B. Admissibility and probative value of modern techniques of authentication

As already indicated, authentication has a probative function.[28] To constitute evidence of a transaction in the event of a dispute concerning its existence or content, authentication should comply with certain requirements.

First, there are the legal requirements (B.1). However, as far as commercial transactions are concerned, such requirements are very limited in Belgian and French private law. To convince the judge in charge of resolving the dispute, the party who insists upon its rights under a transaction should bring convincing evidence of that transaction. Therefore, authentication must also satisfy certain practical requirements of reliability. We will examine how judges have treated new techniques of authentication in light of the few existing cases (B.2).

Finally, we will examine the possibility for parties in a regular business relationship to agree, by way of telematics, on authentication techniques which they want to recognize as having a privileged probative value (B.3).

The legal requirements

Concerning the requirements of the law of evidence, there is a fundamental distinction between a legal fact (*"fait juridique"*) and a legal act (*"acte juridique"*). The former can be proven by any means the law allows (*e.g.*, presumption, oral evidence), but the latter can, in principle, only be proven with a signed written document, as provided for in article 1341, ¶ 1 of the Belgian Civil Code.[29] A legal act can be distinguished from a legal fact on the basis that the legal effects of the former are deliberately sought by its author, and those of the latter are independent of his will.[30]

According to certain writers, the performance of a legal act (*e.g.*, a contract) is to be deemed a legal fact.[31] However, this opinion is controversial.

Telematic transactions can be categorized as legal acts or legal facts. For example, the conclusion of a purchase-sale agreement by way of telematic exchange of messages between the parties constitutes a legal act. However, payment for the goods purchased by an electronic funds transfer should be categorized as a legal fact, to the extent that such payment constitutes the sale-purchase agreement by the buyer.

As a legal act, a telematic transaction is, in principle, subject to the requirement of a signature as contained in article 1341, ¶ 1 of the Belgian Civil Code. The strict interpretation[32] given to this provision, according to which a signature has to be handwritten in order to ensure the physical presence of the person appending it, makes it an obstacle to the use of telematics to conclude legal acts. The main advantage of telematics is to allow the immediate conclusion of legal acts at a distance, without requiring the parties to the acts to be physically present. In certain countries, the legislatures have considered an amendment to the Civil Code to solve this problem. This was the case in the Grand Duchy of Luxembourg, where it was proposed to define the notion of signature in the Civil Code by the following terms:

> "The signature consists of the appending by a person of his name or any other sign whereby such person is individualized and he indicates his agreement."

However, this proposal has not been adopted. The obstacle created by the requirement of article 1341, ¶ 1 of the Belgian Civil Code is largely limited in its effects by paragraph 2 of the same provision. This latter paragraph restricts the scope of paragraph 1 by stating that paragraph 1 is without prejudice to what is provided for in commercial law. Pursuant to commercial law (articles 25 and 109, respectively, of the Belgian and French commercial codes) concerning acts and undertakings which have a commercial character,[33] evidence is not restricted and all forms of evidence are admissible at the discretion of the judge.

Since this article deals with computer-aided commercial transactions, it is not within its purpose to examine the possible difficulties created by dematerialization with regard to article 1341.

Under the principles of evidence applicable in commercial law, all modern techniques of authentication are, in principle, admissible as evidence of commercial transactions. However, there are several exceptions to this principle. For example, in Belgian Law (article 25 of the law of June 11, 1974), the insurance contract should be proven in writing; pursuant to a well-established custom confirmed by the Supreme court, all claims against invoices of an important amount should be expressed in writing. Pursuant to article 3 of the law of October 25, 1919, on the pledge of good will, the validity of the pledge is subject to the existence of a writing.

Although the above-mentioned principle allows the free admissibility of all means of proof,

the judge has the power to evaluate their probative value. One should therefore examine the probative value which can be granted to modern techniques of authentication in existing case law.

Existing case law on new techniques of authentication

The words of an American judge clearly illustrate the issue examined below. In *Perma Research & Development v. Singer Co.*,[34] computer output was admitted by the court. However, one judge said concerning the reliability of this document: "As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ."[35] The difficulty in convincing judges of the reliability of a modern technique of authentication exists both in Anglo-Saxon law and in continental law.[36] However, in the context of this article, we will cite only examples from continental case law.

There are, of course, very few cases concerning the most recent techniques of authentication described above (*e.g.*, cryptography, secret codes, recognition by physical characteristics). Therefore, this analysis refers to other techniques of authentica-tion which are less recent—essentially, those used for transactions performed by telex or telephone.

French case law demonstrates that judges realize that it is now a common business practice to conclude agreements by telex. This appears from the high degree of probative value they have granted to such agreements.[37] In Belgium, there is, to our knowledge, no cases relating to the reliability of telex in commercial matters. This absence of disputes might be an indication of the trust granted by business people to the use of telex.

The Italian example is interesting. Pursuant to the Presidential Decree nº 735 of February 7, 1963, a contract concluded by telex is equivalent to a written contract, provided that (i) the user of the telex identifies himself correctly by giving his telex number and the corresponding code at the end of any communication, and (ii) he keeps a copy of all telexes sent and prohibits the use of his telex installation by third parties. In a judgment by the Tribunal of Ascoli-Pireno,[38] the tribunal held that since a telex message identifies the telex machine which sent the text of the message, and since that machine is at the exclusive disposal of the sender, it is assumed that the latter is the owner of the telex installation. According to the tribunal, this presumption is rebuttable. For example, it can be rebutted on the basis of the invoice from the P.T.T. Since this invoice contains details of the dates, times, and lengths of all telex communications, it could establish, in certain cases, that it was not the owner of the installation who sent the message.

Concerning transactions concluded by telephone, a decision by the French Supreme Court[39] is rather different from the jurisprudence relating to telex contracts discussed above. In this case, a newspaper contended that it received an order by telephone to publish various advertisements. The firm which owned and used the corresponding telephone installation argued that it never ordered those advertisements and refused to pay for them. The Tribunal ordered the firm to pay for those orders, holding that the firm was responsible for the telephone installation, and therefore, should control its use. The Supreme Court quashed this judgment.

One can see that the judges give a high degree of probative value to telex, which is a technique extensively used to conclude commercial transactions. On the other hand, telephones which do not provide the same guarantees of their reliability (no possibility of automatic and safe identification of the sender of the message) do not receive the same degree of probative value.

Agreements on authentication

We have seen from case law that judges give a high degree of probative value to those modern techniques of authentication which are already extensively used in practice.

The probative value which would be given by a court to an even more modern technique of authentication, which is less extensively used (such as cryptography or recognition of physical characteristics), is uncertain. To eliminate this uncertainty, the parties can, on the basis of article 1134 of the Civil Code, agree in writing and in the traditional fashion to give a privileged probative value to the particular technique used in their telematic transactions. Indeed, according to many writers, article 1341 of the Civil Code is neither a mandatory provision nor a public order provision. It would be possible, therefore, to derogate from the written document rule by an evidentiary clause in the agreement stating that legal transactions performed on a telematic system may be proven by specific means.

Such a convention is not conceivable if the parties are not in a regular business relationship. Case law relating to payment instructions by telex[40] indicates that an agreement on authentication would not require the addressee of the message to carry it out (the message received in accordance with the authentication procedure), if it appears from its content and from the circumstances that the message could not have been sent by the authorized sender.

An agreement on authentication, for example, can be included in the contract on electronic cash management between a bank and its customer. Such a provision can also appear in the terms and conditions to which the banks subscribe when they join an electronic funds transfer system or a

system for the communication of financial information. It is important for the parties to agree on the length of time during which they will retain the documents evidencing the authentication techniques used.

Thanks to contractual arrangements, which are permitted by the Civil Code, undertakings to conclude telematic transactions enjoy flexibility concerning the means of authentication, and ensure legal security. Of course, such contractual arrangements are only possible between parties to the underlying contract. However, we believe that once an authentication technique is widely used in the business community, such as the banking sector, it is likely that the technique is reliable and a court, in the absence of an agreement, would give it a privileged probative value.

Part 2 will appear in the November 1988 issue of the International Computer Law Adviser.

Mr. Amory is with the Brussels law firm of Dechert, Price and Rhoads, and is a member of the Adviser's International Editorial Board. Mr. Thunis is Deputy Director of the Centre de Recherches Informatique et Droit, Namur, Belgium.

Footnotes

1. Society for Worldwide Interbank Financial Telecommunications.

2. Concerning the concept of authentication, see Syx, "Naar nieuwe vormen van handterkening? Het probleem van de handtekening in het electronisch rechsverkee," *Kredietbank,* 30 August 1985, nº 10.

3. We will clarify the meaning of this concept below.

4. In this article, we will not use the term "paperless transaction" which appears inadequate since the combined use of computers and telecommunications rarely results in a total disappearance of paper. The fundamental question is, in fact, the following: is the paper generated by these techniques a "writing" having probative value under continental law?

5. Concerning this distinction, see "Legal Value of Computer Records," United Nations Commission on International Trade Law a/CN9 265, at 4.

6. For more details, see "Aspects juridiques de l'échange automatique de donnés commerciales," Nations-Unies, Conseil Economique et Social Trade/WP4/R.185/REV.1 octobre 1982, at 8 *et seq.* and 22 *et seq.*

7. According to M. Van Quickenborne, these are the functions of the signature which, as discussed hereafter, are a type of authentication. See Van Quickenborne, "Quelques réflexions sur la signature des actes sous seing privé," Note sous cass. 28 June 1982, R.C.J.B., 1985, at 57.

8. UNCITRAL, Doc. A/CNO/265 of 21 February 1985, at 16 (free translation by the authors).

9. Before handwriting became popular, authentication was realized through seal or "seeing" (see De Page, "Traité élémentaire de droit civil belge," Brussels, 1967, Vol. III, nr.777).

9bis. Cfr. reference under (8) (free translation by the authors).

10. Van Quickenborne, *supra* note 7.

11. De Page, *supra* note 9, nº 778 and 778 bis.

12. *See, e.g.,* art. 14(4) of the United Nations Convention on the Carriage of Goods by Sea (Hamburg 1978) and art. 5(1) of the Convention On Freight Agreements in International Road Carriage of Goods. Similarly, during the preparatory discussions for the Geneva Convention on Cheque, it has been stressed that the word "signature" refers to any material sign used, along with the habits of the country involved, to identify on papers or documents the person appending (reported by M. Varseur & C. Marni, Le Chèque, Sirey, Paris, 1969, at 100).

13. For more details on telematics and its various aspects, see La Télématique, Technical, Legal and sous-political Aspects, Vol. 1 and 2—Proceeding of the Conference Organized in Namur on December 5 and 6, 1983 by the Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur, Ed. Story-Scientia, Gent, 1984-1985.

14. From a legal standpoint, electronic funds transfer has been defined by D. Syx as "any transfer of funds initiated not by a paper document but by electronic or telematic means," Syx, "Aspects juridiques du mouvement électronique de fonds," *Kredietbank,* Brussels, 1982, at 12-13.

15. For a description of these systems (SAGITTAIRE AND CCMB) see Banque de France, Service de l'Information, Note d'Information nº 63, November 1984.

16. It is noteworthy that if bank C does not provide to its customer, company B, an electronic cash management system, company B will nevertheless be able to access its account at bank C through telematics in the event it is limited to an electronic cash management system of another bank (bank D) which, pursuant to an agreement with bank C, receives information concerning the accounts of a common customer at bank C and retransmits them via telecommunication to company B on behalf of bank C.

17. *See* Syx, *supra* note 2.

18. Schwab & d'Alencon, "L'authentification des personnes," in Proceeding of the international conference organized by OROS in Paris on October 18 and 19, 1984, on "Les terminaux—point de vente—Fraude et sécurité."

19. See in this respect, Schwab & d'Alencon, *supra* note 18.

20. Sometimes this technique only performs the identification function of authentication.

21. In the case of the memory card, this possible thinks to the microprocessor contained within the card. in the case of the magnetic card, this is possible thanks to a decoding device which "compares the code with the one which it calculates pursuant to a precise algorithm from certain data kept on the track of the magnetic card which is introduced." (Syx, "Aspects juridiques du mouvement électronique de fonds," *K.B. Bruxelles,* 1982, at 46.

22. *See* Van Heurck, "L'authentification dans les systèmes informatiques et télématiques," Actes des Journées Notariales à Tournai les 26 et 27 septembre 1985.

23. This definition is based on the definition contained on page 9 of the *Note d'Information,* nº 61 of the Banque de France on SWIFT (March 1984).

24. Syx, "Le transfert électronique de fonds, Le droit hésitant face à une réalité galopante in La Télématique," Actes du Colloque organisé à Namur les 5 et 6 décembre 1983, par le Centre de Recherches informatique et Droit des Facultés Notre-Dame de Namur, vol. 2, Story-Scientia, Gent, 1985, at 244.

25. See, notably, Syx, *supra* note 2, at 246 on the "Security-Key" of the Tell-Link system.

26. Another original example of authentication has just been set up by Belgian banks and it is known as TRASEC. One can find a description of this system in Van Heurck, *supra* note 22.

27. Schwab & d'Alencon, *supra* note 18.

28. *Cfr. supra.*

29. Art. 1341, ¶ 1 of the Belgian Civil Code provides that "any transaction exceeding the amount or the value of three thousand francs should be done under notarial deed or private signature, even for voluntary deposits."

30. For an interesting discussion of the complex notions of legal act and legal fact, see Poullet & Thunis, "Introduction aux aspects juridiques de la télématique," in La Télématique, Aspects techniques, juridiques et socio-politiques, Actes du Colloque organisé à Namur les 5 et 6 décembre 1983 par le Centre de Recherches Informatique et Droit des Facultés Notre-Dame de Namur, Story- Scientia, Gent., 1984, vol. 1, at 159.

31. *See* Catala, "La nature juridique du paiement," Paris, *L.G.D.J.,* 1961.

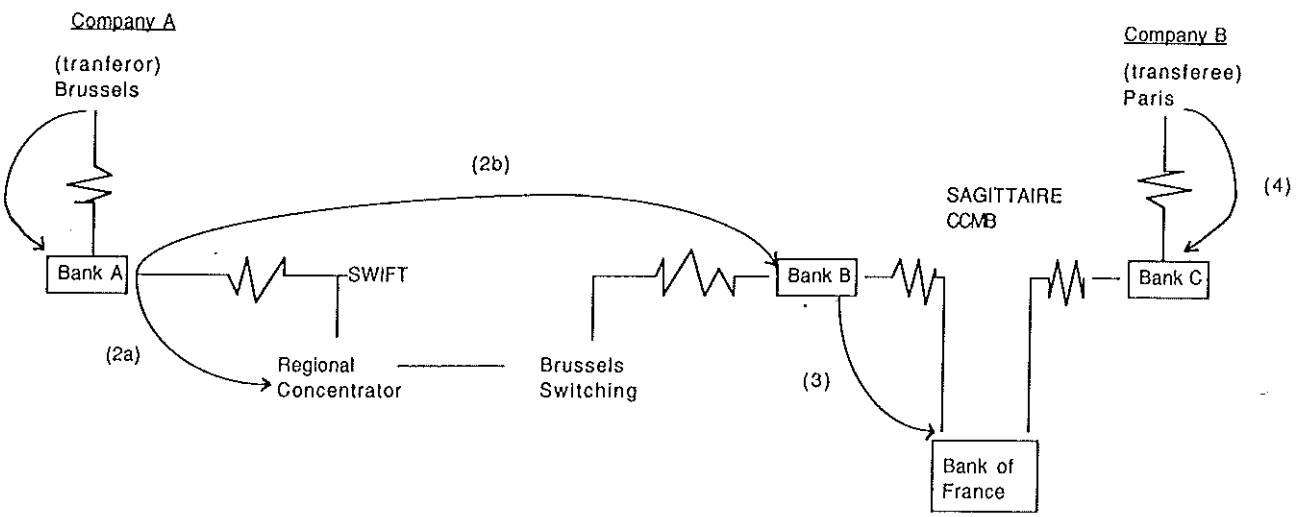
32. See in this respect cass. comm. fr., 19 nov. 1973, Bull. Civ. 1973, nº 3 and Van Quickenborne, *supra* note 7, at 84 and the cited Supreme Court decisions contra, the position adopted by Syx favorable to a functional definition of signature which would permit to include within this notion some modern techniques of authentication (Syx, *supra* note 2).

33. *See* Cass. March 29, 1976, Pas., 1976, II, 833. For more details, see X. Dieux, La preuve en droit commercial, présentation at the I.D.E.F. conference, Brussels 1984.
34. 452 F.2d 11 (2d Cir. 1976).
35. *Id.* (dissenting opinion of Judge Van Graafeiland).
36. *See* Amory & Poullet, "Le droit de la preuve face à l'informatique et à la télématique," *Revue Internationale de Droit Comparé*, 2, 1985, at 331.
37. *See* "Telex contracts, A Comparative Study," *International Fin. L. Rev.*, May 1982, at 22.
38. *Soc. Socoma v. Soc Sider-Tronto*, Tribunale Ascoli Piceno, September 7, 1980, European Commercial Cases, vol. V, July 1982, at 317.
39. *See supra* note 37.
40. *See* Carton, "Aspects juridiques des ordres de virement transmis par telex," *D.I.S.E.P.*, vol. 1, nº 2 october 1985, at 3.

Additional Reading

Amory & Poullet, "Computer Evidence—A Comparative Approach in Civil and Common Law Systems," 1 ICLA, Jan. 1987, at 7 (Part I); 1 ICLA, Feb. 1987, at 12 (Part II).
Niblett, "The Challenge of Presenting Technical Evidence," 2 ICLA, Jan. 1988, at 6.
Potter, "Electronic Filing of Tax Returns," 2 ICLA, Dec. 1987, at 24.

Points of authentification in an international electronic funds transfer



(1) to (4) : points of authentification

PUBLICATIONS

Chinese Trademarks, *by David B. Kay & Lee D. Green* (1988). Published by Shomei, Ltd., M5 New Henry House, 10 Icehouse Street, Hong Kong. 112 pp. $60.00 post-paid.

As more of the Asian continent opens to technology imports and technology transfer agreements, the practical question of choosing and using trademarks for the Chinese consumer becomes extremely important. Just as trademarks are a crucial element of marketing products in the West, the same is true in Chinese-speaking counties. It is for that reason that this book is particularly timely.

This is the second edition of the book and includes a great deal of practical information for anyone attempting to adopt and use trademarks in the PRC, Hong Kong, Taiwan, and other Chinese-speaking area of Asia. It covers selection and usage of trademarks, registration and licensing of trademarks, as well as the legal rights to protect those trademarks in the various jurisdictions. In addition, it includes three appendices on phonetic pronunciation, trademark laws and regulations of the PRC, and the trademark law of Taiwan.

For anyone doing business in Asia, this is an invaluable reference source.